10/069,676

4

PCT/JPC0/05802

28.08.00

8/3

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月２７日

出願番号
Application Number: 平成１１年特許願第２８３２９５号

出願人
Applicant (s): 株式会社デジタル・パブリッシング・ジャパン

JP 00/05802

4

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　９月２９日

特許庁長官
Commissioner,
Patent Office　及川耕造

出証番号　出証特２０００－３０７８７４０

【書類名】　特許願

【整理番号】　0003

【提出日】　平成11年 8月27日

【あて先】　特許庁長官　殿

【発明の名称】　画像の不正使用防止方法

【請求項の数】　3

【発明者】

【住所又は居所】　京都市北区上賀茂本山１９６番地１号

【氏名】　新藤　次郎

【特許出願人】

【住所又は居所】　京都市北区上賀茂本山１９６番地１号

【氏名又は名称】　株式会社デジタル・パブリッシング・ジャパン

【代表取締役】　新藤　次郎

【電話番号】　075-712-5161

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図　面　1

【物件名】　要約書　1

【書類名】　明細書

【発明の名称】画像の不正使用防止方法

【特許請求の範囲】

【請求項１】サーバーからクライアントへの画像配信において、クライアント側の画像処理プログラムが内部メモリに画像表示情報を展開した段階で、画像表示情報そのものに不正防止のためのデータを付加することを特徴とする画像の不正使用防止方法。

【請求項２】請求項目１の動作過程において、クライアント側プログラムが付加した不正防止のためのデータ内容をサーバー側プログラムに送信することにより、クライアント毎の画像使用の記録をサーバーに蓄積し、不正使用が行われた場合に個別画像の流出経路を特定することを可能にすることを特徴とする画像の不正使用防止方法。

【請求項３】デジタル画像の不正使用防止のためにユーザー認識データを、不連続な特定画素に対する輝度の増加または減少によって、画像情報そのもの内部に付加することを特徴とする画像の不正使用防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル画像オンライン配信における不正使用防止技術に関するものである。

【０００２】

【従来の技術】従来のデジタル画像オンライン配信における不正使用防止方法は、あらかじめ配信するデジタル画像の中に画像の出所を明らかにする情報を付加するというものであった。この場合には、画像の不正使用が発見された場合においても、その画像が何時、どのコンピュータに対して、誰の契約アカウントにもとづいて配信されたものであるのか特定することは出来なかった。

【０００３】

【発明が解決しようとする課題】本発明が解決しようとする課題は、オンライン配信されたデジタル画像が不正使用された場合に、その流出経路を特定することを可能にする認識データをデジタル画像に付加し、不正使用防止効果を高めるこ

とである。

【０００４】

【課題を解決するための手段】上記課題を解決するため、本発明では専用のサーバー側プログラムとクライアント側プログラムを用い、サーバーから送信された画像データがクライアント側プログラムによって画像表示情報として内部メモリー上に展開された瞬間に、日時、ユーザーＩＤ、ハードディスクシリアルナンバー、ＩＰアドレス等の認識データを不連続な特定画素に対する輝度の増加（または減少）に転換して画像情報そのものの内部に付加する方式を用いる。

【０００５】

【発明の実施の形態】動作過程としては、クライアント側プログラムは、ネットワーク環境において起動すると同時にサーバー側プログラムに対して認証の要求を行う。サーバー側プログラムは、ユーザーＩＤ、ＩＰアドレス、クライアント側プログラム固有のＩＤとしてのハードディスクシリアルナンバーを確認して認証を与える。

【０００６】

認証されたクライアント側プログラムはサーバー側プログラムに対して画像送信の要求を出すことが出来る。サーバー側プログラムは圧縮された画像ファイルを送信し、クライアント側プログラムはこのファイルを解凍し、画像表示可能な画

【０００７】

この画像情報の展開に続く一連の動作として、クライアント側プログラムは日時、ユーザーＩＤ、ハードディスクシリアルナンバー、ＩＰアドレス等、不正使用防止のための認識データを符号化して不連続な特定画素に対する輝度の増加（または減少）の処理を行う。

【０００８】

クライアント側プログラムは、こうして画像情報そのものの内部に不正使用防止のための認識データを付加すると同時に、画像生成に関する情報をサーバー側プログラムに送信し、サーバー側プログラムはこれをログとして記録する。

【０００９】

クライアント側プログラムは、画素データのマップとしてコンピュータの内部メモリー上に展開され、不正使用防止のための認識データを付加されたデータを、ユーザーの利用形態に応じてディスプレー表示またはファイル出力する。

【００１０】

【発明の効果】本発明においては、不正使用防止のための認識データは画像情報そのものの内部に符号化して保持されるとともに、サーバー側にユーザー固有の画像配信ログ情報として保持されることになる。この方式を用いることにより、画像の不正な利用が発見された場合に、その画像に残存する不正使用防止のための認識データとサーバー側に残されたユーザー固有の画像配信ログを照合することにより、不正利用された画像の流出経路を追跡し特定することが可能となる。

【００１１】

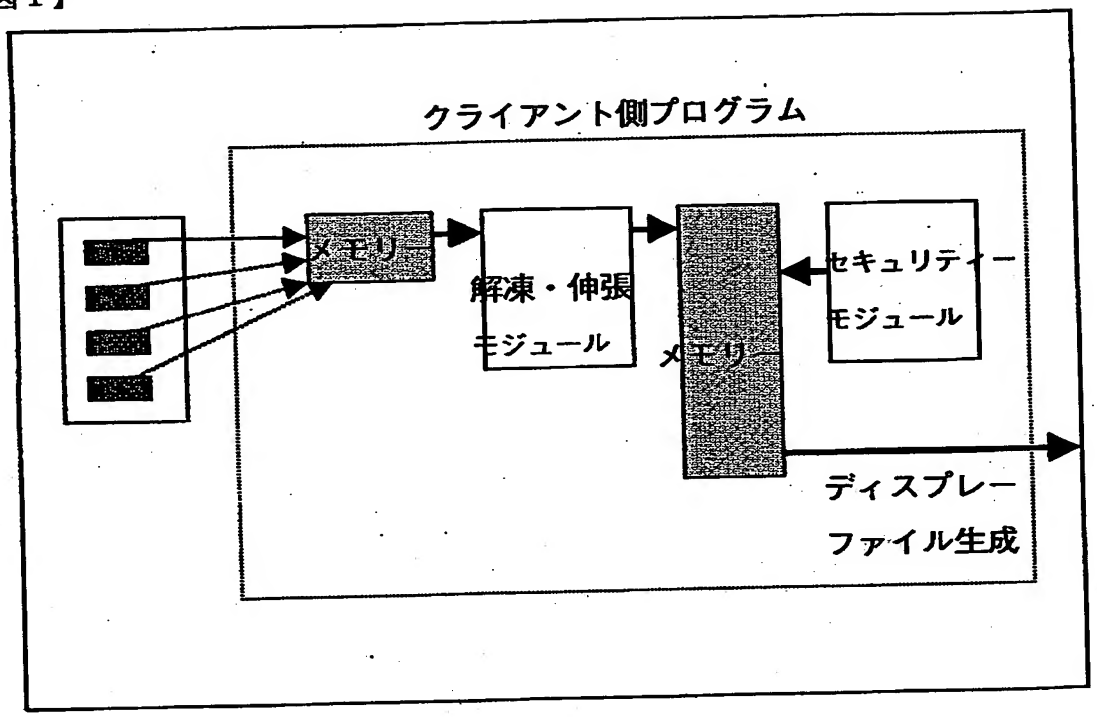
これまでの、画像の出所のみを特定しうる認識データの付加方式に比べ、流出経路が特定される方式は、画像の不正利用を行うものに対してはより強い心理的抑制効果を持つことになる。

【図面の簡単な説明】

【図１】クライアント側プログラム内部における、画像情報に対するの不正使用防止のための認識データ付加プロセスを示す図である。

【書類名】　図面

【図１】


クライアント側プログラム
メモリ
解凍・伸張
モジュール
メモリ
セキュリティー
モジュール
ディスプレー
ファイル生成

【書類名】　要約書

【要約】

【課題】オンライン配信されたデジタル画像が不正使用された場合に、その流出経路を特定することを可能にする認識データをデジタル画像に付加し、不正使用防止効果を高めること。

【解決手段】サーバーから配信された画像データが、クライアント側で画像表示情報に展開された段階で、ユーザー固有の識別が可能な認識情報を符号化し、不連続な特定画素に対する輝度の増加または減少として画像そのものの中に付加する。同時にサーバー側にユーザーへの画像配信ログとして認識情報を記録し、不正使用された画像が発見された場合に、その流出経路を特定できるようにする。

【選択図】図１

出 願 人 履 歴 情 報

識別番号　〔５９９１３９２４６〕

１．変更年月日　１９９９年　８月２７日
［変更理由］　新規登録
住　所　京都市北区上賀茂本山１９６番地１号
氏　名　株式会社デジタル・パブリッシング・ジャパン